M E T U Department of Mathematics

Math 123, Fall 2023, Midterm 1, November 14, 2023, 17:40		
FULL NAME	ID NUMBER	SIGNATURE
8 QUESTIONS ON 4 PAGES		DURATION: 90 MINUTES

Q1.(15 points) Prove that

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) = \frac{n(n+1)(n+2)}{3}$$

for all integers $n \geq 1$.

We shall prove that the statement $(*)$: $1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) = \dfrac{n(n+1)(n+2)}{3}$ holds for all $n \in \mathbb{N}$, by induction on n.

- **Base step.** We have that $1 \cdot 2 = \frac{1 \cdot 2 \cdot 3}{3}$ and hence $(*)$ holds for $n = 1$.
- **Inductive step.** Let $n \geq 1$ be an integer. Assume as inductive hypothesis that $(*)$ holds for n, that is,

  $$1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) = \frac{n(n+1)(n+2)}{3}$$

  It now follows from the inductive assumption that

  $$1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) + (n+1) \cdot (n+2) = \frac{n(n+1)(n+2)}{3} + (n+1)(n+2)$$

  On the other hand, the term on the right hand side equals

  $$\frac{n(n+1)(n+2)}{3} + (n+1)(n+2) = \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{3} = \frac{(n+1)(n+2)(n+3)}{3}$$

  So we have

  $$1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) + (n+1) \cdot (n+2) = \frac{(n+1)(n+2)(n+3)}{3}$$

  Thus $(*)$ holds for $n+1$. Hence, by the principle of mathematical induction, $(*)$ holds for all $n \in \mathbb{N}$.

Q2.(10 points) State the **definition** of **the least common multiple** of two non-zero integers a and b: A positive integer k is said to be the least common multiple of a and b if . . . .

- $a \mid k$ and $b \mid k$; and
- For all positive integers c, if $a \mid c$ and $b \mid c$, then $k \leq c$.

Q3.(15 points) Using the Euclidean algorithm, obtain integers x and y that satisfy the following equality: $\gcd(430, 185) = 430x + 185y$.

Applying the Euclidean algorithm, we obtain that

$$\begin{aligned} 430 &= 185 \cdot 2 + 60 \\ 185 &= 60 \cdot 3 + 5 \\ 60 &= 5 \cdot 12 + 0 \end{aligned}$$

Since the last non-zero remainder is 5, we know that $\gcd(430, 185) = 5$. Starting from the last equation and writing the remainders of previous equations in the reverse order, we get that

$$\begin{aligned} 5 &= 185 + 60 \cdot (-3) \\ 5 &= 185 + (430 + 185 \cdot (-2)) \cdot (-3) = 185 \cdot 7 + 430 \cdot (-3) \end{aligned}$$

Thus, choosing $x = -3$ and $y = 7$, the equation $\gcd(430, 185) = 430x + 185y$ is satisfied.

Q4.(10 points) If exists, find all the integer solutions of the linear Diophantine equation $15x + 35y = 140$. If such a solution does not exist, explain why this is the case.

Observe that $\gcd(15, 35) = 5 \mid 140$. Thus, by a theorem proven in class, the linear Diophantine equation $15x + 35y = 140$ has a solution. In order to obtain all solutions, we first need to find a particular solution. By trial-and-error, we see that $x_0 = 0$ and $y_0 = 4$ is a particular solution of this equation. Therefore, by the same theorem referred above, we obtain that

$$x = x_0 + \frac{35}{\gcd(15, 35)} t = 7t \text{ and } y = y_0 - \frac{15}{\gcd(15, 35)} = 4 - 3t \text{ where } t \text{ ranges over } \mathbb{Z}$$

gives all solutions to this linear Diophantine equation

FULL NAME	ID NUMBER	SIGNATURE

Q5.(15 points) Without using Dirichlet's theorem, prove that there are infinitely many prime numbers of the form $4n+3$.

Assume towards a contradiction that there are finitely many primes of the form $4n+3$, say, $q_1, q_2, \ldots, q_k$ is the list of all primes of the form $4n+3$. Consider the number

$$N = 4 \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_k - 1 = 4 \cdot (q_1 \cdot q_2 \cdot \cdots \cdot q_k - 1) + 3$$

By the Fundamental Theorem of Arithmetic, we can write N as $N = r_1 \cdot r_2 \cdot \ldots r_m$ where r_i's are prime numbers. Observe that N is odd since N is of the form $4n+3$. Therefore, r_i is an odd prime and so is of the form $4n+1$ or $4n+3$ for every $1 \leq i \leq m$. We next argue that not all of r_i's can be of the form $4n+1$.

Recall that a product of numbers of the form $4n+1$ is of the form $4n+1$. Therefore, if it **were** that r_i of the form $4n+1$ for every $1 \leq i \leq m$, then N would be of the form $4n+1$, which is not the case. It follows that r_j is of the form $4k+3$ for **some** $1 \leq j \leq m$.

Since r_j is a prime number of the form $4k+3$, it appears in the list $q_1, q_2, \ldots, q_k$ and hence $r_j \mid 4 \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_k$. But then, since $r_j \mid N$ as well, we obtain that

$$r_j \mid N - (4 \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_k) = -1$$

This leads to a contradiction as the only divisors of -1 are 1 and -1.

Q6.(10 points) Verify that 283 is a prime number.

Observe that $16 < \sqrt{283} < 17$. Therefore, to check that 283 is a prime number, it suffices to divide 283 by all prime numbers less than 17 and see whether 283 is divisible by any of these. The prime numbers less than 17 are $2, 3, 5, 7, 11, 13$. Dividing 283 by these numbers, we obtain that

$$283 = 2 \cdot 141 + 1$$
$$283 = 3 \cdot 94 + 1$$
$$283 = 5 \cdot 56 + 3$$
$$283 = 7 \cdot 40 + 3$$
$$283 = 11 \cdot 25 + 8$$
$$283 = 13 \cdot 21 + 10$$

If 283 were not prime, then it would have a factor that is less than or equal to $\sqrt{283}$ other than 1; but this factor itself would have a prime factor. Thus, if 283 were not prime, then it would have a prime factor that is less than or equal to $\sqrt{283}$. We have already checked that 283 does not have a prime factor that is less than or equal to $\sqrt{283}$, so it must be a prime number itself.

Q7.(10 points) Show that $123^{123} + 33$ is divisible by 60.

By computing the first few powers of 123 modulo 60, we obtain that

$$\begin{aligned} 123^1 &\equiv 3^1 \equiv 3 \pmod{60} \\ 123^2 &\equiv 3^2 \equiv 9 \pmod{60} \\ 123^3 &\equiv 3^3 \equiv 27 \pmod{60} \\ 123^4 &\equiv 3^4 \equiv 21 \pmod{60} \\ 123^5 &\equiv 3^5 \equiv 3 \pmod{60} \end{aligned}$$

It follows that

$$123^{123} \equiv 3^{123} \equiv (3^5)^{24} \cdot 3^3 \equiv 3^{24} \cdot 3^3 \equiv 3^{27} \equiv (3^5)^5 \cdot 3^2 \equiv 3^5 \cdot 3^2 \equiv 3^7 \equiv 3^5 \cdot 3^2 \equiv 3 \cdot 3^2 \equiv 27 \pmod{60}$$

Consequently, we have

$$123^{123} + 33 \equiv 27 + 33 \equiv 60 \equiv 0 \pmod{60}$$

This means that the remainder of $123^{123} + 33$ when it is divided by 60 is 0, that is, $123^{123} + 33$ is divisible by 60.

Q8.(15 points) Let a, b be integers and $n \geq 2$ be an integer such that $\gcd(a + b, n) = 1$. Prove that if $a^2 \equiv b^2 \pmod{n}$, then $a \equiv b \pmod{n}$.

Assume that $a^2 \equiv b^2 \pmod{n}$. Then, by the properties of congruence, by subtracting b^2 from both sides, we obtain that $a^2 - b^2 \equiv 0 \pmod{n}$ and so $(a - b)(a + b) \equiv 0 \pmod{n}$. Since we have $\gcd(a+b, n) = 1$, by a theorem proven in class, we can cancel the factor $a+b$ from both sides of a congruence relation modulo n and consequently, we have $a - b \equiv 0 \pmod{n}$. This implies that $a \equiv b \pmod{n}$.

Alternative solution. Assume that $a^2 \equiv b^2 \pmod{n}$. Then, by the properties of congruence, by subtracting b^2 from both sides, we obtain that $a^2 - b^2 \equiv 0 \pmod{n}$ and so $(a - b)(a + b) \equiv 0 \pmod{n}$. Thus $n \mid (a - b)(a + b)$. Since we have $\gcd(a + b, n) = 1$, by a lemma proven in class, we have that $n \mid (a - b)$ and hence $a - b \equiv 0 \pmod{n}$. This implies that $a \equiv b \pmod{n}$.